# NUTANIX Cyber Security on Nutanix at Nutanix Brandon.Gagliardi@Nutanix.com 2019

MAY 2019 | CONFIDENTIAL



- Brandon Gagliardi
- Sr. Security Engineer

## My 1st Week at Nutanix

- Drink our own champagne.
- Lean IT team.
- Major deliverables in a short time.

|3

## "Here's your home page where you can monitor resources" – Platform team

Hypervisor Summary	Prism Central	Cluster-wide Controller IOPS	2,051 IOPS	Health		Critical Alerts		
AHV 2 VERSIONS ⑦	OK 10.40.64.85 Launch	2:00 PM 3:00 F	PM 4:00 PM	CRITICAL				
Storage Summary	Logical 👻	Cluster-wide Controller IO B/W	77.72 MBps	Remote Sites • 1 • 0 • 0				
10.19 TiB free (logical) of 22.84 TiB		2:00 PM 3:00 I	PM 4:00 PM	Services • 1	• 0 • 0	No Crit	ical Alerts	
		2.00 PM 5.00 P		VMs • 0	• 1 • 47			
VM Summary		Cluster-wide Controller Latency	8.29 ms	Data Resiliency Status		Warning Alerts		
48 VM(S)	AvailabilityBest Effort• On41• Off7• Suspend0• Paused0	2:00 PM 3:00 F	PM 4:00 PM	OK		WARNING 14 hours ago	Remote site connectivity not normal. PE-PC Connection Failure Detected older AHV Version License Node Invalid	
Hardware Summary		Cluster CPU Usage	Cluster Memory Usage	Data Resiliency possible		Info Alerts	Events	
5 2 HOSTS BLOCKS	NX-3060-G5	<b>27.61</b> % OF 335.92 GHz	57.6 % of 1.23 tib	<ul> <li>Rebuild capacity available</li> </ul>	YES	No Info Alerts	722 EVENTS Last event 6 minutes ago	

## "...Here's The Template – This is your environment."

Overview • Table												+ Create VM	Network Co
VM									Include Control	er VMs · 2 VMs (filtere	d from 48) · · < > · :	🗘 🗸 · 🛛 :entOS7	_x64-Template
<ul> <li>VM Name</li> </ul>	Host	IP Addresses	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write	Controller IO Bandwidth	Controller Avg IO Latency	Backup and	Flash Mode
CentOS7_x64-Template			2	2 GiB	1.82 GIB / 524 GIB	0%	0%	-			•	Yes	No
<ul> <li>CentOS7_x64- Template_another_pass</li> </ul>			2	2 GiB	2.26 GiB / 12 GiB	0%	0%	а	140	-	-	Yes	No
		Update VM		? ×					Update VM	? ×			
	or Timezone			26									
	(UTC) UTC		Clu	ister -			0	DISK scsi.0	SIZE=2GiB; CONTAINE	ER= / · ×			
	□ Lise this VM as an ar	ient VM					0	DISK scsi.1	SIZE=10GiB; CONTAIN	NER 🗡 · 🗙			
							0	DISK scsi.2	SIZE=512GiB; CONTAI	NE 💉 🗙			
	Compute Details												
	VCPU(s)						Volum	ne Groups					
	2							You haven't a	added any volume group	is vet			
	Number Of Cores Per Vcpu								in the second second second				
	1								Add Volume Group				
	Memory												
	2			GIB			Netwo	ork Adapters (NIC)					
								Ver her					
	Disks		+ Add Ne	ew Disk				rou nav	en tadded any NICs yet.				
	BOOT	RESS PARAMETERS							+ Add New NIC			_	_
				-									
	1		Close	Save						Close			

## Infrastructure Created in Minutes for Splunk

- First workload on Nutanix for Corp Cyber Security
- 7 VM's
- Unique allocations of vCPU & memory per server based on Splunk best practices
- Whole environment stood up in 30minutes.
- (BTW Dedicated vCPU's.)

|6

## **Environment Unexpected Growth**

90GiB/day	4 Nodes	August 2017
200GiB/day	4 Nodes	December 2017*
500GiB/day	8 Nodes	April 2018
1TiB/day	12 Nodes	October 2018

## Fun Stuff Happened Along The Way

What happened to my node? Doh!

| 8

## Problems Don't Occur When It's Convenient

The alert condition for 'DMC Alert - Critical System Physical Memory Usage' was triggered.

Alert: DMC Alert - Critical System Physical Memory Usage

#### View results in Splunk

Instance	Memory used (%)	Memory used (MB)	Physical memory installed (MB)
drt-itsec-indexer-prod-2.corp.nutanix.com	95.0	22722.438	23913.102

The alert condition for 'DMC Alert - Search Peer Not Responding' was triggered.

Alert: DMC Alert - Search Peer Not Responding

#### View results in Splunk

Instance	Status
drt-itsec-indexer-prod-1.corp.nutanix.com:8089	Down
drt-itsec-universalforwarder-prod-1.corp.nutanix.com:8089	Down

.

## Onboarded 30 New Security Analysts Concurrent Searches Went Up

The alert condition for 'DMC Alert - Critical System Physical Memory Usage' was triggered.

Alert: DMC Alert - Critical System Physical Memory Usage

#### View results in Splunk

Instance	Memory used (%)	Memory used (MB)	Physical memory installed (MB)
drt-itsec-indexer-prod-2.corp.nutanix.com	95.0	22722.438	23913.102

The alert condition for 'DMC Alert - Search Peer Not Responding' was triggered.

Alert: DMC Alert - Search Peer Not Responding

#### View results in Splunk

Instance	Status
drt-itsec-indexer-prod-1.corp.nutanix.com:8089	Down
drt-itsec-universalforwarder-prod-1.corp.nutanix.com:8089	Down

.

## Data Center Migrations Fluxes in Firewall Data (+50% Daily Ingest Spikes)

The alert condition for 'DMC Alert - Near Critical Disk Usage' was triggered.

Alert: DMC Alert - Near Critical Disk Usage

#### View results in Splunk

Instance	Mount Point	File System Type	Capacity (GB)	Usage (GB)	Usage (%)
drt-itsec-indexer-prod-1.corp.nutanix.com	/data	xfs	7095.48	6522.44	91
drt-itsec-indexer-prod-2.corp.nutanix.com	/data	xfs	7095.48	6418.80	90
drt-itsec-indexer-prod-3.corp.nutanix.com	/data	xfs	6072.00	5564.31	91

## Time to Remediate and Validate Problem Start to Finish w/ Distractions: Less than 15 Minutes

Overview · Table							
∨м							
<ul> <li>VM NAME</li> </ul>	HOST	IP ADDRESSES	CORES	MEMORY CAPACITY	STORAGE	CPU USAGE	MEMORY USAGE
drt-itsec-indexer-prod-1	NTNX-Block-1-C/AHV	10.4.8.170	20	24 GiB	6.93 TiB / 6.94 TiB	1.09%	99.93%
drt-itsec-indexer-prod-2	NTNX-18SM6F140180- C/AHV	10.4.8.171	20	24 GiB	6.89 TIB / 6.94 TIB	81.13%	99.31%
drt-itsec-indexer-prod-3	NTNX-18SM6F140180- A/AHV	10.4.204.24	20	24 GiB	5.69 TIB / 5.94 TIB	92.85%	97.42%
drt-itsec-indexer-prod-4	NTNX-Block-1-A/AHV	10.4.204.25	20	24 GiB	5.13 TIB / 5.94 TIB	93.04%	98.25%

### Shut VM Down and Give it More Power

	24 GIB	6.89 TIB / 6	94 TIB	0.57%	15.22%	_	198
	Power of	fVM				? X	1254
	Select the	type of power of	f action:				1432
	O Power	off					0
	O Power	cycle					
	○ Reset						0
	Guest	Shutdown					0
	⊖ Guest	Reboot	h	ţ.			0
							0
					Cancel	Submit	0
2					manage oues	a 10015 - 20	Laun

DESCRIPTION	
This is a base template to clone from	
TIMEZONE	
(UTC) UTC	•
Use this VM as an agent VM	
Compute Details	
VCPU(S)	
20 I	
NUMBER OF CORES PER VCPU	
1	
MEMORY	
24	GIB
Disks	+ Add New Disk

(UTC)	UTC			•
Use	this VM as a	n agent VM		
Compute	e Details			
VCPU(S)				
24				
NUMBER	OF CORES PE	R VCPU		
1				
MEMORY				
32				GiB
Disks				+ Add New Disk
BOOT DEVICE	TYPE	ADDRESS	PARAMETERS	
$\bigcirc$	CD-ROM	ide.0	EMPTY=true; BUS=ide	$\mathbb{A} \times \mathbb{Z} \times \mathbb{X}$

## Time to Give it More Storage to Handle the New Amounts of Data: No Reboot Required

Update	• VM			?	×	Add Disk		? >	:	Add Disk		?	×
						TUDE				TYPE			
VCPU(S)						TYPE			14	DISK			*
24						DISK		Ŷ		OPERATION			
NUMBER OF CORES PER VCPU					OPERATION			13					
1						Allocate on Storage Container 🗸				Bus Submitting operation to create virtual disk for VM drt- itsec-indexer-prod-2.			
MEMODY						BUS TYPE			- 12	sc	S		Ľ
				CIP		SCSI 🗸				STOR			-
3Z GIB				GID									
					1.1	STORAGE CONTAINER				1000			
					-	default-container-93924		•					
Disks				+ Add New Di	sk	SIZE (GIB)				Next Available			~
ROOT				0		1000							
DEVICE	TYPE	ADDRESS	PARAMETERS			INDEX						Cancel	Add
0	CD-ROM	ide 0	EMPTY=true: BUS=ide	A . Z . X		Next Available		v					
<u> </u>	00 110111	100.0		_ , ,,									
0	DISK	scsi.0	SIZE=2GiB; CONTAINER=def	1 · ×			Cancel	Add					
0	DISK	scsi.1	SIZE=10GiB; CONTAINER=def	1 · ×								0.00 110 1 010	
0	DISK	scsi.2	SIZE=1000GiB; CONTAINER=	2 · ×			NTNX-18SM6F140180-						
						drt-itsec-indexer-prod-2	CAHV	10.4.8.17	1	24	32 GIB	6.89 TiB / 7.92	2 TIB
				Close	ave		GIATIV						
12.		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~ ~ ~ ~ ~								•		

## **Upgrade Complete**

Overview · Table					
VM					
	LIGST		00055		5700405
<ul> <li>VM NAME</li> <li>drt-itsec-indexer-prod-1</li> </ul>	NTNX-Block-1-C/AHV	10.4.8170	24	32 GiB	6.95 TIB / 7.92 TIB
<ul> <li>drt-itsec-indexer-prod-2</li> </ul>	NTNX-18SM6F140180- C/AHV	10.4.8.171	24	32 GIB	6.9 TIB / 7.92 TIB
drt-itsec-indexer-prod-3	NTNX-18SM6F140180- A/AHV	10.4.204.24	24	32 GiB	5.7 TIB / 6.92 TIB
drt-itsec-indexer-prod-4	NTNX-Block-1-B/AHV	10.4.204.25	24	32 GiB	5.13 TiB / 6.92 TiB

## Workloads Hosted On Nutanix by CyberSec Team To Date

- Splunk
- Rapid7 Console & Scanners
- OpenVAS
- Phantom
- Web Server/IPAM
- Skybox Firewall Assurance

- Intsights Threat Intel
- Exabeam UBA
- Burp Enterprise
- Fyde Zero Trust
- Kenna Security Connector
- HA Proxies
- Fos Wiki

## Questions?

## Automating Containment on Nutanix with Phantom

## My Story

- Nick Pierini
- Manager, Security Engineering
- Splunk Phantom user for 3+ years

## Nutanix Phantom App Intro



Nutanix Prism

Publisher: Nutanix

This app implements the virtualization actions for Nutanix Prism

#### 

- **test connectivity** Validate the asset configuration for connectivity using supplied configuration
- get system info Get information about a VM
- list vms Get the list of registered VMs
- revert vm Revert VM to specified snapshot
- snapshot vm Take a snapshot of the VM
- start vm Start a stopped or suspended VM
- stop vm Stop a VM
- suspend vm Suspend a VM (Requires guest tools installed on vm)
- search vms Query VM's based on string
- list snapshots List snapshots in a cluster
- get snapshot info Get information of a specific snapshot
- I1 Associated Playbooks

### Demo

### Questions

| 22